FULL CONTENTS

[Claim(s)]

[Claim 1] From one side of two pieces of the data transmission-and-reception equipment mutually connected by ad hoc wireless connection, send the data for verification data generation to another side, and [one data transmission-and-reception equipment] Make the verification data generated based on the 1st generation algorithm from the transmitted data for verification data generation output to one's verification data output section, and [the data transmission-and-reception equipment of another side] The verification data generated based on said 1st generation algorithm from the received data for verification data generation is made to output to one's verification data output section. The verification system for ad hoc wireless communications characterized by judging whether the verification data in the verification data output section of both data transmission-and-reception equipment is mutually in agreement.

[Claim 2] Said verification data is a verification system for ad hoc wireless communications according to claim 1 characterized by being visual or hearing verification data.

[Claim 3] It is the verification system for ad hoc wireless communications according to claim 1 characterized by outputting verification data by the output form of both visual and hearing in the detected information output section.

[Claim 4] The input of this operator and the result of an operation of this operator are defined for the numeric value on which an operator and this operator act a function as the output of this operator. The in-series operator sequence which put in order in series one or more same or different operators which start a tropism function on the other hand is prepared. The verification system for ad hoc wireless communications according to claim 1 to 3 characterized by using the input of this in-series operator sequence as the data for verification data generation, and using the output or its correspondence value of this in-series operator sequence as verification data.

[Claim 5] Said 1st generation algorithm is what generates two or more verification data. The

verification system for ad hoc wireless communications according to claim 1 to 3 characterized by judging whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.
[Claim 6] The input of this operator and the result of an operation of this operator are defined for the numeric value on which an operator and this operator act a function as the output of this operator. The in-series operator sequence which put in order in series two or more same or different operators which start a tropism function on the other hand is prepared. Use the input of this in-series operator sequence as the data for verification data generation, and the output or its correspondence value of two or more operators chosen from all the operators which constitute this in-series operator sequence is used as verification data, respectively. The verification system for ad hoc wireless communications according to claim 5 characterized by judging whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.
[Claim 7] The input of this operator and the result of an operation of this operator are defined for the numeric value on which an operator and this operator act a function as the output of this operator. Prepare two or more operators which are mutually different and which start a tropism function on the other hand, and the data for verification data generation is considered as the common input of each operator. The verification system for ad hoc wireless communications according to claim 5 which uses the output or its correspondence value of each operator as verification data, respectively, and is characterized by judging whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.
[Claim 8] It is the verification system for ad hoc wireless communications according to claim 1 to 7 characterized by said data for verification data generation being the public key of one data transmission-and-reception equipment.
[Claim 9] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function by said ad hoc wireless-communications verification system to the personal digital assistant with a wireless communication function of the user of another side is verified From a personal digital assistant with a wireless communication function, a public key Kp is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal computer with a wireless

communication function] Based on the information transmitted using the code by a public key from the personal computer with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. The personal computer with both wireless communication functions is a data transmission-and-reception system for ad hoc wireless communications using the verification system for ad hoc wireless communications according to claim 8 characterized by sending and receiving data in the code based on a common key Kc henceforth.

[Claim 10] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function by said ad hoc wireless-communications verification system to the personal digital assistant with a wireless communication function of the user of another side is verified [the personal digital assistant with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal digital assistant with a wireless communication function] Based on the information transmitted using the code by a public key from the personal digital assistant with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. Next, from a personal digital assistant with a wireless communication function, a common key Kc is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with both wireless communication functions] Henceforth, the data transmission-and-reception system for ad hoc wireless communications using the verification system for ad hoc wireless communications according to claim 8 characterized by sending and receiving data in the code based on a common key Kc.

[Claim 11] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function to the personal digital assistant with a wireless communication function of the user of another side is verified From a personal digital assistant with a wireless communication function, a public key Kp is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with a wireless communication function of the user of another side] Based on the 2nd generation algorithm, generate a common key Kc from a public key Kp, and

[one user's personal computer with a wireless communication function] Based on the information transmitted using the code by a public key from the personal computer with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. The personal computer with both wireless communication functions is a data transmission-and-reception system for ad hoc wireless communications characterized by sending and receiving data in the code based on a common key Kc henceforth.

[Claim 12] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function to the personal digital assistant with a wireless communication function of the user of another side is verified [the personal digital assistant with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal digital assistant with a wireless communication function] Based on the information transmitted using the code by a public key from the personal digital assistant with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. Next, a common key Kc is a data transmission-and-reception system for ad hoc wireless communications which is transmitted to a personal computer with a wireless communication function from a personal digital assistant with a wireless communication function in each user, and is characterized by the personal computer with both wireless communication functions sending and receiving data in the code based on a common key Kc henceforth.

[Claim 13] From one side of two pieces of the data transmission-and-reception equipment mutually connected by ad hoc wireless connection, send the data for verification data generation to another side, and [one data transmission-and-reception equipment] Make the verification data generated based on the 1st generation algorithm from the transmitted data for verification data generation output to one's verification data output section, and [the data transmission-and-reception equipment of another side] The verification data generated based on said 1st generation algorithm from the received data for verification data generation is made to output to one's verification data output section. The verification method for ad hoc wireless communications characterized by judging whether the verification data in the verification data output section of both data transmission-and-reception equipment is mutually in agreement.

[Claim 14] Said verification data is the verification method for ad hoc wireless communications according to claim 13 characterized by being visual or hearing verification data.

[Claim 15] It is the verification method for ad hoc wireless communications according to claim 13 characterized by outputting verification data by the output form of both visual and hearing in the detected information output section.
[Claim 16] The input of this operator and the result of an operation of this operator are defined for the numeric value on which an operator and this operator act a function as the output of this operator. The in-series operator sequence which put in order in series one or more same or different operators which start a tropism function on the other hand is prepared. The verification method for ad hoc wireless communications according to claim 13 to 15 characterized by using the input of this in-series operator sequence as the data for verification data generation, and using the output or its correspondence value of this in-series operator sequence as verification data.
[Claim 17] Said 1st generation algorithm is what generates two or more verification data. The verification method for ad hoc wireless communications according to claim 13 to 15 characterized by judging whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.
[Claim 18] The input of this operator and the result of an operation of this operator are defined for the numeric value on which an operator and this operator act a function as the output of this operator. The in-series operator sequence which put in order in series two or more same or different operators which start a tropism function on the other hand is prepared. Use the input of this in-series operator sequence as the data for verification data generation, and the output or its correspondence value of two or more operators chosen from all the operators which constitute this in-series operator sequence is used as verification data, respectively. The verification method for ad hoc wireless communications according to claim 17 characterized by judging whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.
[Claim 19] The input of this operator and the result of an operation of this operator are defined for the numeric value on which an operator and this operator act a function as the output of this operator. Prepare two or more operators which are mutually different and which start a tropism function on the other hand, and the data for verification data generation is considered as the common input of each operator. The verification method for ad hoc wireless communications according to claim 17 which uses the output or its correspondence value of each operator as verification data, respectively, and is characterized by judging whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.
[Claim 20] It is the verification method for ad hoc wireless communications according to claim 13 to 19 characterized by said data for verification data generation being the public key of one data transmission-and-reception equipment.

[Claim 21] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function by said ad hoc wireless-communications verification system to the personal digital assistant with a wireless communication function of the user of another side is verified From a personal digital assistant with a wireless communication function, a public key Kp is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal computer with a wireless communication function] Based on the information transmitted using the code by a public key from the personal computer with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. The personal computer with both wireless communication functions is the data transmission-and-reception method for ad hoc wireless communications of using the verification method for ad hoc wireless communications according to claim 20 characterized by sending and receiving data in the code based on a common key Kc, henceforth.

[Claim 22] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function by said ad hoc wireless-communications verification system to the personal digital assistant with a wireless communication function of the user of another side is verified [the personal digital assistant with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal digital assistant with a wireless communication function] Based on the information transmitted using the code by a public key from the personal digital assistant with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. Next, from a personal digital assistant with a wireless communication function, a common key Kc is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with both wireless communication functions] Henceforth, the data transmission-and-reception method for ad hoc wireless communications of using the verification method for ad hoc wireless communications according to claim 20 characterized by

sending and receiving data in the code based on a common key Kc.
[Claim 23] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function to the personal digital assistant with a wireless communication function of the user of another side is verified From a personal digital assistant with a wireless communication function, a public key Kp is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with a wireless communication function of the user of another side] Based on the 2nd generation algorithm, generate a common key Kc from a public key Kp, and [one user's personal computer with a wireless communication function] Based on the information transmitted using the code by a public key from the personal computer with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. The personal computer with both wireless communication functions is the data transmission-and-reception method for ad hoc wireless communications characterized by sending and receiving data in the code based on a common key Kc henceforth.
[Claim 24] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function to the personal digital assistant with a wireless communication function of the user of another side is verified [the personal digital assistant with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal digital assistant with a wireless communication function] Based on the information transmitted using the code by a public key from the personal digital assistant with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. Next, a common key Kc is the data transmission-and-reception method for ad hoc wireless communications which is transmitted to a personal computer with a wireless communication function from a personal digital assistant with a wireless communication function in each user, and is characterized by the personal computer with both wireless communication functions sending and receiving data in the code based on a common key Kc henceforth.

[Claim 25] The record medium which recorded the program for verification systems of the following contents for ad hoc wireless communications.
: From one side of two pieces of the data transmission-and-reception equipment mutually connected by ad hoc wireless connection, send the data for verification data generation to another side, and [one data transmission-and-reception equipment] Make the verification data generated based on the 1st generation algorithm from the transmitted data for verification data generation output to one's verification data output section, and [the data transmission-and-reception equipment of another side] The verification data generated based on said 1st generation algorithm from the received data for verification data generation is made to output to one's verification data output section, and it is judged whether the verification data in the verification data output section of both data transmission-and-reception equipment is mutually in agreement.
[Claim 26] The record medium according to claim 25 which recorded the program for verification systems of the following contents for ad hoc wireless communications.
: Said verification data is visual or hearing verification data.
[Claim 27] The record medium according to claim 25 which recorded the program for verification systems of the following contents for ad hoc wireless communications.
: Verification data is outputted by the output form of both visual and hearing in the detected information output section.
[Claim 28] The record medium according to claim 25 to 27 which recorded the program for verification systems of the following contents for ad hoc wireless communications.
: Define the input of this operator, and the result of an operation of this operator for the numeric value on which an operator and this operator act a function as the output of this operator. The in-series operator sequence which put in order in series one or more same or different operators which start a tropism function on the other hand is prepared, use the input of this in-series operator sequence as the data for verification data generation, and let the output or its correspondence value of this in-series operator sequence be verification data.
[Claim 29] The record medium according to claim 25 to 27 which recorded the program for verification systems of the following contents for ad hoc wireless communications.
: Said 1st generation algorithm generates two or more verification data, and has it judged whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.
[Claim 30] Distribution equipment which distributes the program for verification systems of the following contents for ad hoc wireless communications.
: From one side of two pieces of the data transmission-and-reception equipment mutually connected by ad hoc wireless connection, send the data for verification data generation to another side, and [one data transmission-and-reception equipment] Make the verification data

generated based on the 1st generation algorithm from the transmitted data for verification data generation output to one's verification data output section, and [the data transmission-and-reception equipment of another side] The verification data generated based on said 1st generation algorithm from the received data for verification data generation is made to output to one's verification data output section, and it is judged whether the verification data in the verification data output section of both data transmission-and-reception equipment is mutually in agreement.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] The verification system for ad hoc wireless communications with which this invention copes with the alteration of transmission data, It is related with the data transmission-and-reception system for ad hoc wireless communications, the verification method for ad hoc wireless communications, the data transmission-and-reception method for ad hoc wireless communications, the record medium that recorded the program of correspondence and that is reached and distributed, and distribution equipment.
[0002]
[Description of the Prior Art] When two unspecified persons transmit without a holder in bad faith altering data in the temporary short-distance-radio communication which does not use a specific infrastructure like ad hoc wireless communications, it is necessary to share the cryptographic key which is not in being known by the holder in bad faith. However, the method of setting up the value which serves as a basis of the cryptographic key at any time at the time of communication is complicated, and the thing in particular for which communications partners exchange [a communications partner] cryptographic keys by oral, a memorandum, etc. under situations, such as the first meeting, is almost impractical. There is a way share a public key first, and the public key enciphers and shares a cryptographic key as a method of sharing a cryptographic key automatically. However, the Mann Inn THE middle attack (Man-in-the-middle attack: [details / of the Mann Inn THE middle attack]) The title of author blues SHUNAIA (BRUCE SCHNEIER) of John Willie and Suns company (John Wiley & Sons, Inc) publication : [p.48 to p.50 of application cryptography (APPLIED CRYPTOGRAPHY)] Please refer to it. There is a risk.
[0003] The outline of the risk of the data alteration in the Mann Inn THE middle attack is carried out. Drawing 1 shows the room to which holder-in-bad-faith C intervenes among both while a transmission destination B has not noticed the transmitting agency A in the ad hoc radio communications system 10. As shown in (a), if the channel is directly established among both,

even if it considers A and B, as shown in (b), in fact, the third party may be interrupting below them among both. "Man-in-the-Middle Attack" mentions concretely how it performs, and explains an example.

[0004] The general procedure of radio cryptocommunication way establishment is as follows.

Procedure 1: Appeal for a transmitting agency toward many and unspecified partners by ID of a transmission destination which wants to communicate.

Procedure 2: If a transmission destination is in the range in which wireless connection is possible, the ID (that is, its ID) for which it appealed will be received.

Procedure 3: Tell a transmission destination to transmitting [a self operating condition etc.] origin.

Procedure 4: Determine parameters [required for channel establishment] (selection of a channel, a setup, exchange of a cryptographic key to be used) of operation in both.

Procedure 5: Channel establishment is carried out and mutual communication is started.

[0005] What a holder in bad faith enters the position of C of drawing 1 to easiliest is timing to which two persons who are the targets of tapping start wireless communications by meeting. That is, it intervenes in the enumerated above-mentioned procedures 1-3. Drawing 2 and drawing 3 show an example of a means for a holder in bad faith to enter the position of C of drawing 1 . The transmitting agency A obtains an appeal colander by Specification ID for no surrounding transmission destination candidates on the character of an electric wave (Procedure 1). Since the appeal in its ID can be heard (Procedure 2), a transmission destination B answers the transmitting agency A (Procedure 3). Here, a holder in bad faith answers the appeal to IDs other than himself, or performs appeal by IDs other than himself, and tries to plan the following **********. First, holder-in-bad-faith C throws the noise of the same frequency band at the response of a transmission destination B, and the transmitting agency A is prevented from catching the response. At this time, since a transmission destination B does not know the fact of that noise, it changes for the above-mentioned procedure 4, and is waiting for the session start in Procedure 4 from the transmitting agency A. Since the transmitting agency A is not in Procedure 4, a transmission destination B returns to the state of hearing the appeal of one's ID again after a time-out. On the other hand, since the response from a transmission destination B is not obtained, the transmitting agency A has that common for which it appeals by the ID again same after a time-out (Procedure 1). That is, the transmitting agency A and a transmission destination B will notice the failure by each time-out, and will return to the original state noting that they will begin to take the synchronization of a mutual procedure.

[0006] The transmitting agency A stands by according to the timing for which it appeals by the same ID again, and holder-in-bad-faith C stands by also according to the timing which a transmission destination B begins to hear further that the appeal of its ID is again. Henceforth,

it performs appeal with it. [in the disguise of / it answers the appeal of the transmitting agency A with holder-in-bad-faith C in the disguise of a transmission destination B, and / the transmitting agency A / the transmission destination B which began to hear the appeal of its ID on the contrary] Of course, holder-in-bad-faith C is preparing the capacity to change one's ID to any IDs. since it is not identical time that a transmission destination B returns [transmitting agency A] from a gap to the original state above in the synchronization of a mutual procedure -- such two -- it can become completely and holder-in-bad-faith C can perform an act. It is because the time when a transmission destination B begins to stand by in the following event the transmitting agency A, respectively differs primarily, the events which are the targets of a time-out also differ, so the timeout periods itself differ.

[0007] this -- [it becomes completely, and / with work / the agency / the transmitting agency A thinks that there was a normal response from the regular transmission destination B, and] From the channel establishment procedure 4, i.e., a procedure, it changes together with holder-in-bad-faith C, and a transmission destination B thinks that it is the appeal from the regular transmitting origin A, and changes together with [it is same with a channel establishment procedure, and] a third party C. It becomes possible to intercept in the form where holder-in-bad-faith C relays communication data in between [mutual], without being known by the holder of Both A and B device currently regarded as having secured the channel only by two persons when it progressed to the above-mentioned procedure 5. this -- becoming completely (relay) -- if it uses, C can alter the public key which A should send to B, for example, and it can substitute for the public key corresponding to the secret key which C prepared beforehand secretly. By this, the cryptocommunication way originally built between A and B becomes effective only between A and C, and it becomes the cryptocommunication way which C set up independently between C and B. That is, the encryption data sent from A is decrypted by C, and again, another encryption is applied for the encryption communication ways between C and B to it, and it is transmitted to it. The reverse transmission is also the same. Having usually established the encryption communication way in the procedure, both A and B are a public key's being substituted secretly on the way, and not noticing the substitution, and bring a result intercepted. Such an attack (tapping depended for becoming completely) is called Man-in-the-middle attack. Since the encryption communication way itself is safe, it becomes important [ensuring whether both who communicate are sharing the really same public key as dealing with such an attack].

[0008]

[Problem to be solved by the invention] As for transmission-individuals ID (usually partner's name etc.) indicated in certificate origin, as ways of coping of Man-in-the-middle attack, displaying and carrying out a visual comparison at a transmission place is also considered using the certificate which an authentication authority publishes. However, cost starts issue of

a certificate at this. Moreover, when using an authentication authority, in order to attest by registering an identity, its identity will be opened to a communications partner and the problem that anonymity cannot be maintained also exists. Furthermore, when using the service which specifies a user from a public key like a yellow page (Yellow Page), the secure network connection by the telephone line etc. is required, and transaction cost starts.
[0009] [when the purpose of this invention sends and receives data between the data transmission-and-reception equipment mutually connected by ad hoc wireless connection] The verification system for ad hoc wireless communications which can prevent effectively the alteration of the data based on spoofing to a communications partner, It is offering the data transmission-and-reception system for ad hoc wireless communications, the verification method for ad hoc wireless communications, the data transmission-and-reception method for ad hoc wireless communications, the record medium that recorded the program of correspondence and that is reached and distributed, and distribution equipment. Other purposes of this invention can omit an exchange of the password by oral or memorandum writing. The verification system for ad hoc wireless communications which cannot use the authentication authority which does identity public presentation, but can verify a communications partner efficiently, smoothly, and correctly, It is offering the data transmission-and-reception system for ad hoc wireless communications, the verification method for ad hoc wireless communications, the data transmission-and-reception method for ad hoc wireless communications, the record medium that recorded the program of correspondence and that is reached and distributed, and distribution equipment.
[0010]
[Means for solving problem] According to the verification system for ad hoc wireless communications and method of this invention, the data for verification data generation is sent to another side from one side of two pieces of the data transmission-and-reception equipment mutually connected by ad hoc wireless connection. The verification data generated with one data transmission-and-reception equipment based on the 1st generation algorithm from the transmitted data for verification data generation is made to output to one's verification data output section. Moreover, the verification data generated with the data transmission-and-reception equipment of another side based on the 1st generation algorithm from the received data for verification data generation is made to output to one's verification data output section. It is judged whether the verification data in the verification data output section of both data transmission-and-reception equipment is mutually in agreement.
[0011] Since the distance of both data transmission-and-reception equipment needs to contrast the verification data in the verification data output section of both data transmission-and-reception equipment mutually, it is less than 10 etc.m with which a user (user) can keep company between both data transmission-and-reception equipment in several seconds

typically, and is several meters preferably. Suppose at the verification data generated based on the data for verification data generation that you may be the data for verification data generation itself. Verification data is set as what the judgment of whether the verification data in the detected information output section of both data transmission-and-reception equipment is mutually in agreement tends to perform. If the software for verification started in both data transmission-and-reception equipment is generally the same, the generation algorithm same for generation of the data for verification data generation to verification data will be used. However, the user of both data transmission-and-reception equipment decides on one in two or more generation algorithms suitably on the spot.

[0012] One data transmission-and-reception equipment generates verification data based on the 1st generation algorithm from the transmitted data for verification data generation. The data transmission-and-reception equipment of another side generates verification data based on the 1st generation algorithm from the received data for verification data generation. And [judge whether the verification data outputted from the detected information output section of both data transmission-and-reception equipment is in agreement, and] if in agreement It means that being correctly transmitted to the data transmission-and-reception equipment of another side from one data transmission-and-reception equipment, i.e., a data integrity, was verified, without altering the data for verification data generation on the way. Thus, a data integrity is efficiently verifiable.

[0013] According to the verification system for ad hoc wireless communications and method of this invention, verification data is visual or hearing verification data.

[0014] A picture, a numeric value, characters, or those combination are in visual verification data. As an example of a vision display of verification data, when verification data is a total of n-bit bit data, n bit is classified by every [a bit, such as continuing,], and there is a histogram which considers as a Type to x axial direction, and is made into the quantity for every Type to y axial direction. As an example of a hearing display of verification data, the sound of the height corresponding to the quantity of each Type of the above-mentioned histogram is outputted in an order from the Type of lower order. As for verification data, it is desirable that that a user tends to judge smoothly and correctly the coincidence and the inequality of verification data in both data transmission-and-reception equipment to be is chosen.

[0015] According to the verification system for ad hoc wireless communications and method of this invention, verification data should be outputted by the output form of both visual and hearing in the detected information output section.

[0016] According to the visual output form of verification data, even if the things in both data transmission-and-reception equipment are similar, by the hearing output form of verification data, a difference is clear or that case of being reverse exists. The accuracy of coincidence and an inharmonious judgment increases by contrasting both the visual output form of

verification data, and a hearing output form.

[0017] According to the verification system for ad hoc wireless communications and method of this invention, a function An operator, The input of this operator and the result of an operation of this operator are defined for the numeric value on which this operator acts as the output of this operator. The in-series operator sequence which put in order in series one or more same or different operators which start a tropism function on the other hand is prepared, use the input of this in-series operator sequence as the data for verification data generation, and let the output or its correspondence value of this in-series operator sequence be verification data.

[0018] On the other hand, there is a hash function (Hash Function) in a tropism function. The operator also contains the thing only with one piece in the operator sequence which gave [above-mentioned] the definition. By on the other hand making a tropism function participate in generation of the verification data from the data for verification data generation The difficulty which finds out the data for verification data generation from verification data increases, and a possibility that a holder in bad faith will do a data alteration using the data for verification data generation of a false similar to the true data for verification data generation falls. In addition, the more serial arithmetic child queue length becomes long, the more it becomes impossible in computational complexity to find out the data for verification data generation from verification data.

[0019] According to the verification system for ad hoc wireless communications and method of this invention, the 1st generation algorithm generates two or more verification data, and has it judged whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.

[0020] A possibility that two or more verification data of all is similar is very low. The accuracy of verification improves by generating two or more verification data and judging whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.

[0021] According to the verification system for ad hoc wireless communications and method of this invention, a function An operator, The input of this operator and the result of an operation of this operator are defined for the numeric value on which this operator acts as the output of this operator. The in-series operator sequence which put in order in series two or more same or different operators which start a tropism function on the other hand is prepared. Use the input of this in-series operator sequence as the data for verification data generation, and the output or its correspondence value of two or more operators chosen from all the operators which constitute this in-series operator sequence is used as verification data, respectively. It is judged whether about each verification data, the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement.

[0022] According to the verification system for ad hoc wireless communications and method of

this invention, a function An operator, The input of this operator and the result of an operation of this operator are defined for the numeric value on which this operator acts as the output of this operator. Prepare two or more operators which are mutually different and which start a tropism function on the other hand, and the data for verification data generation is considered as the common input of each operator. The output or its correspondence value of each operator is used as verification data, respectively, and it is judged whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.

[0023] According to the verification system for ad hoc wireless communications and method of this invention, the data for verification data generation is the public key of one data transmission-and-reception equipment.

[0024] If the data for verification data generation is the public key of one data transmission-and-reception equipment, it is verifiable that the public key which the data transmission-and-reception equipment of another side received is a public key of one data transmission-and-reception equipment with verification of verification data. Therefore, it carries out sending a common key etc. to one data transmission-and-reception equipment from the data transmission-and-reception equipment of another side by the cryptocommunication using the public key of one data transmission-and-reception equipment etc., and cryptocommunication by the common key between both data transmission-and-reception equipment can be established completely.

[0025] [according to the data transmission-and-reception system for ad hoc wireless communications and method of this invention of using the above-mentioned verification system for ad hoc wireless communications] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function by an ad hoc wireless-communications verification system to the personal digital assistant with a wireless communication function of the user of another side is verified From a personal digital assistant with a wireless communication function, a public key Kp is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal computer with a wireless communication function] Based on the information transmitted using the code by a public key from the personal computer with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm, and data is henceforth sent

[the personal computer with both wireless communication functions] and received in the code based on a common key Kc.

[0026] [according to the data transmission-and-reception system for ad hoc wireless communications and method of this invention of using the above-mentioned verification system for ad hoc wireless communications] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function by an ad hoc wireless-communications verification system to the personal digital assistant with a wireless communication function of the user of another side is verified [the personal digital assistant with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal digital assistant with a wireless communication function] Based on the information transmitted using the code by a public key from the personal digital assistant with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. Next, data is henceforth sent [a common key Kc is transmitted to a personal computer with a wireless communication function from a personal digital assistant with a wireless communication function in each user, and / the personal computer with both wireless communication functions] and received in the code based on a common key Kc.

[0027] [according to the data transmission-and-reception system for ad hoc wireless communications and method of this invention] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function to the personal digital assistant with a wireless communication function of the user of another side is verified From a personal digital assistant with a wireless communication function, a public key Kp is transmitted to a personal computer with a wireless communication function in each user, and [the personal computer with a wireless communication function of the user of another side] Based on the 2nd generation algorithm, generate a common key Kc from a public key Kp, and [one user's personal computer with a wireless communication function] Based on the information transmitted using the code by a public key from the personal computer with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm, and data is henceforth sent [the personal computer with

both wireless communication functions] and received in the code based on a common key Kc.

[0028] [according to the data transmission-and-reception system for ad hoc wireless communications and method of this invention] The personal digital assistant with a wireless communication function and the personal computer with a wireless communication function which are owned by each user exist. It is connected with the channel with each user's secure personal digital assistant with a wireless communication function and personal computer with a wireless communication function. If having been transmitted without altering one user's public key Kp from one user's personal digital assistant with a wireless communication function to the personal digital assistant with a wireless communication function of the user of another side is verified [the personal digital assistant with a wireless communication function of the user of another side] From the 2nd generation algorithm, generate a common key Kc and [one user's personal digital assistant with a wireless communication function] Based on the information transmitted using the code by a public key from the personal digital assistant with a wireless communication function of the user of another side, a common key Kc is generated from the 2nd generation algorithm. Next, data is henceforth sent [a common key Kc is transmitted to a personal computer with a wireless communication function from a personal digital assistant with a wireless communication function in each user, and / the personal computer with both wireless communication functions] and received in the code based on a common key Kc.
[0029] The secure channel of each user's personal digital assistant with a wireless communication function and a personal computer with a wireless communication function is established by the two way communication by each user's secret key, for example. The personal digital assistant with a wireless communication function contains what is called PDA (Personal Digital Assistant). Hiding computing (Hidden Computing: explain the form of implementation of invention in full detail) as an example of the style of work of a businessman is considered. In hidden computing, transmission and reception of data are wanted to be performed, for example without an alteration in personal computers with a wireless communication function, such as Note PC. [a user] in such a case if having been transmitted to the personal digital assistant with a wireless communication function of another side is verified without altering the public key Kp of one personal digital assistant with a wireless communication function on the way from contrast of the verification data in the verification data output section of a personal digital assistant with a wireless communication function The verification is made to take over to both users' personal computer with a wireless communication function, and cryptocommunication can be smoothly carried out with a common key Kc between personal computers with both wireless communication functions.
[0030] The program which the record medium and distribution equipment of this invention record and distribute, respectively is the thing of the following contents.

: From one side of two pieces of the data transmission-and-reception equipment mutually connected by ad hoc wireless connection, send the data for verification data generation to another side, and [one data transmission-and-reception equipment] Make the verification data generated based on the 1st generation algorithm from the transmitted data for verification data generation output to one's verification data output section, and [the data transmission-and-reception equipment of another side] The verification data generated based on the 1st generation algorithm from the received data for verification data generation is made to output to one's verification data output section, and it is judged whether the verification data in the verification data output section of both data transmission-and-reception equipment is mutually in agreement.

[0031] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further. Recording media.

: Verification data is visual or hearing verification data.

[0032] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further.

: Verification data is outputted by the output form of both visual and hearing in the detected information output section.

[0033] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further.

: Define the input of this operator, and the result of an operation of this operator for the numeric value on which an operator and this operator act a function as the output of this operator. The in-series operator sequence which put in order in series one or more same or different operators which start a tropism function on the other hand is prepared, use the input of this in-series operator sequence as the data for verification data generation, and let the output or its correspondence value of this in-series operator sequence be verification data.

[0034] As for the program which the record medium and distribution equipment of this invention record and distribute, respectively, the thing of the following contents is added further.

: The 1st generation algorithm generates two or more verification data, and has it judged whether the things in the verification data output section of both data transmission-and-reception equipment are mutually in agreement about each verification data.

[0035]

[Mode for carrying out the invention] The form of implementation of invention is hereafter explained with reference to Drawings. Drawing 4 is the flow chart of the whole code data

transmission following verification and it of a data integrity. The cryptocommunication open request side and a requestor side are defined as a transmitting agency and a transmission place, respectively, and A and transmission place data transmission-and-reception equipment are set to B for transmitting agency data transmission-and-reception equipment in drawing 4 . [the transmission origin of the public key for data-integrity verification and a transmission place, and the transmission origin of this transmission after data-integrity verification (that is / ******** / right : code transmission using a common key) and a transmission place] It does not need to be in agreement, and it may be reverse and a transmitting agency and a transmission place may interchange suitably in this transmission after data-integrity verification.

[0036] Processing of drawing 4 is explained in order.

(a) A transmits ID (this ID is hereafter called "ID1".) which specifies its public key Kp and verification data generation algorithm as B with a cryptocommunication way open request. A generates the verification data Xp simultaneously based on its own public key Kp.

(b) B sets to Kx the data received as a public key Kp of A to A. If there is no alteration of data in the radio transmission line from A to B, it will become Kx=Kp, and if there is an alteration, Kx will become what has another Kp. B generates the verification data Xx with the verification data generation algorithm of ID1 with the specification [A] with origin of Kx received from A. The example of verification data is explained in full detail in below-mentioned drawing 5 .

(c) The user of A and B verifies whether the verification data Xp by which it was indicated by the output, respectively, and Xx are the same to the display of A and B. If it is Xp=Xx, a judgment that Kx=Kp is meant and there is a data integrity in the channel of A-B will be made.

(d) B enciphers ID (this ID is hereafter called "ID2".) which specifies the random number value R and common key generation algorithm for common key generation using the public key Kp received from A, and transmits to A. About ID2, if ID2 are being fixed, the transmission between A-B can omit like ID1 that A and B use the same communications software etc. B generates a common key Kc using a common key generation algorithm from the random number value R simultaneously.

(e) A decodes the enciphered random number value R which was received from B using the secret key corresponding to a public key Kp, acquires the random number values R and ID2, and generates a common key Kc using the common key generation algorithm of ID2 from the random number value R.

(f) A-B sends and receives data by the encryption communication based on a common key Kc henceforth.

[0037] The verification data displayed on the verification data output section of A and B may be the data for verification data generation (for example, the public key of A itself) itself. That is, fatbits of the public key of A is carried out to the data for verification data generation of A and B. However, numerically, since it is hard to read, you may change the digital readout of a

public key into image display. Drawing 5 shows the histogram as an example of the verification data generated from the data for verification data generation. A vision indication of the verification data is given at the verification image display section 27 of data transmission-and-reception equipment 20 (drawing 6). That the data for verification data generation is the public key of A, a public key is divided into the zone of the number of bits equal in from LSB to MSB in order, and verification data is expressed with the histogram which makes a horizontal axis a zone and makes a vertical axis the quantity of each zone. Since the data Kx for verification data generation which the public key Kp of A became completely by the holder in bad faith in the middle of the transmission line, and B received from A when there was no **** crack **** is equal to the data Kp for verification data generation, it serves as Xx=Xp.
[therefore, the user of A and/or B or other verification persons who can trust it] If the display of A and B is seen directly, Xp and Xx which are displayed on the display of A and B are contrasted (comparison) and both are in agreement It judges that the public key of A has been transmitted to B as it is from A, namely, judges that there is a data integrity, and if both are inharmonious, it will be judged that there was an alteration of data in the middle of transmission to B from A.
[0038] However, the difference from the small similar public key of a humming distance may be undetectable only by generating simply the comparison picture of a histogram like [the precision of man's recognition capacity is not necessarily high, and] drawing 5 . Then, to a public key, on the other hand, a hash function etc. may change into predetermined data with the application of a tropism function, and may display verification pictures, such as a histogram, for it. In this case, even if it is going to ask for another public key which outputs the data with which the third party who tries to perform ********** is similar, a problem logarithmic [discrete] will be solved and it is impossible in computational complexity. However, the amount of information of the verification picture to create may be broken by exhaustive search, when very small compared with the bit size of a public key. Under such conditions, to the data which already applied the tropism function on the other hand, new data is computed, or, further on the other hand, new data is computed with the application of another one-way nature function to a public key with the application of a tropism function, and another verification picture is generated. Two or more verification pictures can be generated and the intensity which receives becoming completely by using this can be raised with repeating this operation.
[0039] Verification data is not limited to a picture like a histogram, but may be shown to a user, and combining two or more of those data. [using the display of alphabetic data, change of a scale, etc.] As hearing verification data, the value of the vertical axis direction of the histogram of drawing 5 is made to correspond to the height or the tone of sound, and the sound corresponding to the value of each zone is outputted to turn for every predetermined time from the zone on the left of the direction of a horizontal axis of drawing 6 . Moreover, you may make

it make verification data output from both a vision drop and the loudspeaker as a sound emission means.

[0040] Drawing 6 - drawing 8 show the method which generates verification data from the data for verification data generation on the other hand using a tropism function, respectively. Data D1 means the data for verification data generation, and data D2, D3, D4, and ... mean verification data. Moreover, an one directivity each function functions as an operator, acts on an input, and outputs the result of an operation. On the other hand, a tropism function is a hash function (Hash Function).

[0041] In drawing 6 , a time, on the other hand, the 1st time makes the tropism function F act on the data D1 as data for verification data generation, and data D2 is obtained. The loop which the same one-way nature function F is made to act on data D2, namely, contains the tropism function F on the other hand is formed, and the 2nd data D3 is obtained. Henceforth, loop processing is repeated and D4, D5, and ... are obtained. After repeating the loop of the number of times of predetermined, the final result of an operation is set to Dn, this Dn is used as verification data, and this verification data is indicated by vision at the verification image display section 27 of data transmission-and-reception equipment 20 (drawing 10). Only the final result of an operation Dn not only indicates by vision, but [the result of an operation / the verification image display section 27 of data transmission-and-reception equipment 20] It may be made to make the verification image display section 27 of data transmission-and-reception equipment 20 indicate some of D2, D3, D4, specific ..., or all by vision by screen separation or time sharing, and you may contrast about each which was displayed. Even if the coincidence about those one verification data and an inharmonious judgment are confusing by contrasting two or more verification data A possibility that coincidence and an inharmonious judgment will become confusing about two or more verification data of all contrasted is very small, and can improve the accuracy of the verification about a data alteration.

[0042] In addition, when D2, D3, D4, and ... all do not come out and it contrasts specific [some of], the protection intensity to a holder's in bad faith attack becomes high by changing the combination (Subset) about the some suitably.

[0043] In drawing 7 , prepare two or more one-way nature functions F, G, and H which are mutually different, and ..., the one directivity each function F, G, and H and ... are made to act on the common data D1, and each result of an operation D2, D3, D4, and ... are obtained. It contrasts about each which the verification image display section 27 of data transmission-and-reception equipment 20 was made to indicate by vision, and was displayed on it by screen separation or time sharing by using some of D2, D3, D4, specific ..., or all as verification data.

[0044] In drawing 8 , two or more one-way nature functions F, G, and H which are mutually different, and ... are prepared. A time, on the other hand, the 1st time makes the tropism function F act on the data D1 as data for verification data generation, and data D2 is obtained.

A time, on the other hand, the 2nd time makes the tropism function G act on data D2, and data D3 is obtained. In this way, the one-way nature function of the next step is made to act on the result of an operation of the preceding paragraph one after another, and two or more D2, D3, D4, and ... are obtained. It contrasts about each which the verification image display section 27 of data transmission-and-reception equipment 20 was made to indicate by vision, and was displayed on it by screen separation or time sharing by using some of D2, D3, D4, specific ..., or all as verification data. In addition, two or more methods of contrast can be considered to be the special examples which use the same one-way nature function F instead of [in drawing 6 / which is mutually different in the method of drawing 8] on the other hand using a tropism function.

[0045] Drawing 9 is the block diagram showing the method which asks for verification data combining processing of drawing 6 - drawing 8 . Drawing 6 - the verification data computing type of drawing 9 are defined as type (Type)1, and 2 and 3, respectively. The data for verification data generation is inputted into the left end of drawing 8 , and verification data is outputted to the right end of drawing 8 . The example of an array of drawing 9 can choose two or more types from Types 1, 2, and 3 which are examples, can arrange them in arbitrary order, and can obtain the data for verification data generation.

[0046] Drawing 10 is the block diagram of data transmission-and-reception equipment 20. data transmission-and-reception equipment 20 became the transmitting agency A by the case, and became the transmission place B -- since it carries out, the composition as a transmitting agency and the composition as a transmission place are combined. When data transmission-and-reception equipment 20 is A, [the transmission verification section 24] The public key of A which outputted its own public key to the verification image generation section 26, and received as a transmitted and received data 31 from A in the communications department 25 when data transmission-and-reception equipment 20 was B is sent to the verification image generation section 26 via the transmission verification section 24. The verification image generation section 26 generates verification data from the public key which received from the transmission verification section 24, and the generated verification data is displayed on the verification image display section 27. Users, such as an owner of A and B, contrast the verification data in the verification image display section 27 of two pieces of the data transmission-and-reception equipment 20 by which ad hoc wireless connection is carried out, investigate coincidence and an inequality, and input the result into the verification result input section 28. The input result to the verification result input section 28 from a user is notified to the transmission verification section 24, and it is judged that the transmission verification section 24 has a data integrity about the public key transmitted to B through the transmission line of ad hoc wireless connection from A when a notice that both verification data is mutually in agreement is received. Next, when data transmission-and-reception equipment 20 is B, a

random number value is generated in the random number generation section 34, and the common key generation algorithm of ID2 generates a common key in the common key generation section 33 from the random number value generated in the random number generation section 34. On the other hand, random number value and ID2 which the random number generation section 34 generated are enciphered based on the public key of A in decoding / encryption implementation section 32, and the code data Dc is sent to A through the transmitted and received data 31. Moreover, based on the generation algorithm of ID2, a common key is generated from the random number value R, and it is saved in the key preservation section 35. When data transmission-and-reception equipment 20 is A, the transmitted and received data 31 of the code data Dc transmitted from B is decoded with its own secret key in decoding / encryption implementation section 32. The random number values R and ID2 are acquired, a common key is generated based on the common key generation algorithm of ID2 from the random number value R, and this common key is saved in the key preservation section 35. When transmitting data, a common key is pulled out from the key preservation section 35, transmit data is enciphered in decoding / encryption implementation section 32 based on this common key, and it transmits to the other party as a transmitted and received data 31 henceforth. it received, when data was received -- it is enciphered and the transmitted and received data 31 is decoded in decoding / encryption implementation section 32, the Taira data is saved at a hard disk (not shown) etc., or predetermined processing is performed.

[0047] Drawing 11 is the flow chart of the communications processing by the side of the transmitting agency A. A public key Kp is transmitted (S40), the verification data generation algorithm of ID1 generates the verification data Xp from this public key Kp (S42), and the verification data Xp is outputted to the verification image display section 27 (S44). In S46, if their own verification data Xp and the verification data Xx of the transmission place B are contrasted and it is judged that it is the same, it will progress to S48, and if it is judged that it is inharmonious, this program will be ended as an error (a data integrity is not accepted). Although it progressed to S52 and the random number value receiving latency time carried out predetermined time progress, when there was a data integrity and it judged that reception of the random number value R from the transmission place B received the random number value R in waiting (S48) and S50 When there is no reception of the random number value R, this program is ended as an error. In S52, the code data of the random number value R from the transmission place B is decoded with its secret key, and the random number value R is acquired. [of correspondence in said public key Kp] Between the data transmission-and-reception equipment of A and B, it decides on ID beforehand about two or more common key generation algorithms, respectively, and ID (an example ID2) adopted as this common key generation algorithm in the transmission destination B has been transmitted to the transmitting

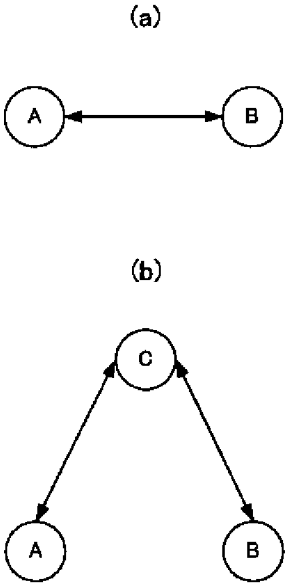
agency A from the transmission place B together with the random number value R. In this way, in S56, based on the common key generation algorithm of ID2, the common key for communication with a transmission destination B is generated from the random number value R, and B and encryption communication are henceforth started using this common key (S58).
[0048] Drawing 12 is the flow chart of the communications processing by the side of the transmission place B. A public key Kx is received from the transmitting agency A (S60). Since the holder in bad faith may intervene between the transmission lines between A and B and may be altered, this received public key is made to express it as Kx instead of Kc. Next, the verification data generation algorithm specified by ID1 sent together with a public key Kp from the transmitting agency A generates the verification data Xx from Kx (S62), and the verification data Xx is outputted to the verification image display section 27 (S64). In S66, if their own verification data Xx and the verification data Xp of the transmitting agency A are contrasted and it is judged that it is the same, it will progress to S68, and if it is judged that it is inharmonious, this program will be ended as an error (a data integrity is not accepted). When there is a data integrity, generate the random number value R (S68), and The random number value R The data which enciphered ID2 as an ID of the selected common key generation algorithm with the public key of the transmitting agency A out of two or more common key generation algorithms this time is transmitted to the transmitting agency A (S70). A common key Kc is generated according to the common key generation algorithm of ID2 (S72), and A and encryption communication are henceforth started using this common key (S74).
[0049] Drawing 13 is an explanatory view which establishes the cryptocommunication way of ad hoc wireless connection among the users whom it hides and a computing style uses. Hide and [computing / (Hidden Computing)] A user dedicates a computer to a bag etc. and means the form of use which operate this computer by remote control using wireless communications etc. from portable devices, such as PDA (Personal Digital Assistant: Personal Digital Assistant) at hand. 82 with which PDA80a etc. is equipped is a communication device. [when performing ad hoc wireless communications between the devices (notebook computers 88a and 88b in the = bags 86a and 86b) which have not equipped the system which can check the data integrity of a public key which was described above] A cryptocommunication way is indirectly established using PDA80a which mounted the cryptocommunication way establishment protocol which has secured the secure channels 90a and 90b to these notebook computers 88a and 88b and beforehand, and 80b. In addition, the secure channel between PDA and a notebook computer is attained by the cryptocommunication by the common key on which it decides in advance, for example among both. In drawing 13 , a channel 84 is first established between PDA80a and 80b in a procedure (a), the public key of one PDA is transmitted to PDA of another side, and the data integrity of this public key is verified. Next, in a procedure (b), the data-integrity verification between PDA80a and 80b is inherited to the notebook computers 88a

and 88b connected with each PDA80a and 80b by the secure channels 90a and 90b. Specifically, this succession is attained by transmitting notebook computers 88a and 88b through the secure channels 90a and 90b in the public key which had the data integrity verified between PDA80a and 80b. Henceforth, after sharing a common key through the channel 92 between both, data is sent [notebook computers 88a and 88b] and received in the code by this common key.

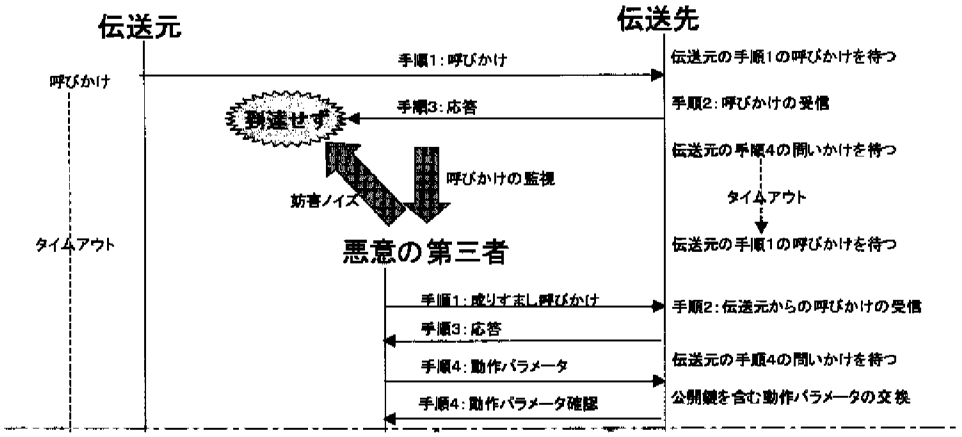
[Brief Description of the Drawings]
[Drawing 1] It is the figure showing the room to which holder-in-bad-faith C intervenes among both while a transmission destination B has not noticed the transmitting agency A.
[Drawing 2] It is the figure showing the 1st portion of an example of a means for a holder in bad faith to enter the position of C of drawing 1 .
[Drawing 3] It is the figure showing the 2nd portion of an example of a means for a holder in bad faith to enter the position of C of drawing 1 .
[Drawing 4] It is the flow chart of the whole code data transmission following verification and it of a data integrity.
[Drawing 5] It is the figure showing the histogram as an example of the verification data generated from the data for verification data generation.
[Drawing 6] It is the figure showing the 1st method which generates verification data from the data for verification data generation on the other hand using a tropism function.
[Drawing 7] It is the figure showing the 2nd method which generates verification data from the data for verification data generation on the other hand using a tropism function.
[Drawing 8] It is the figure showing the 3rd method which generates verification data from the data for verification data generation on the other hand using a tropism function.
[Drawing 9] It is the block diagram showing the method which asks for verification data combining processing of drawing 6 - drawing 8 .
[Drawing 10] It is the block diagram of data transmission-and-reception equipment.
[Drawing 11] It is the flow chart of the communications processing by the side of the transmitting agency A.
[Drawing 12] It is the flow chart of the communications processing by the side of the transmission place B.
[Drawing 13] It is the explanatory view which establishes the cryptocommunication way of ad hoc wireless connection among the users whom it hides and a computing style uses.
[Explanations of letters or numerals]
10 Ad Hoc Radio Communications System

80a, 80b PDA (Personal Digital Assistant with a wireless communication function)
88a, 88b Notebook computer (personal computer with a wireless communication function)

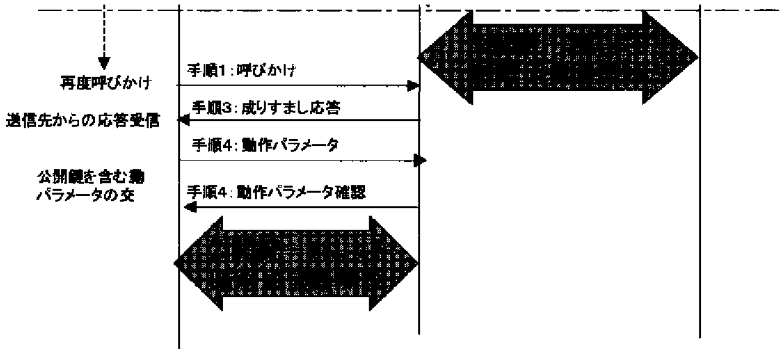
[Drawing 1]



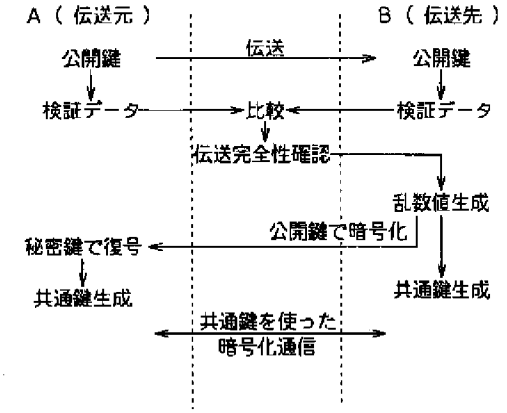
[Drawing 2]



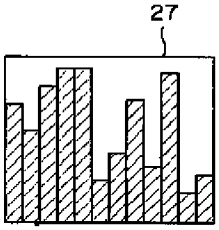
[Drawing 3]



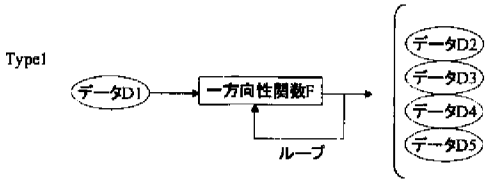
[Drawing 4]



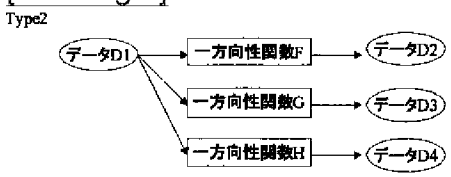
[Drawing 5]



[Drawing 6]

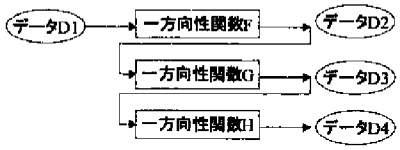


[Drawing 7]

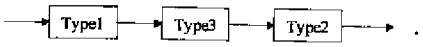


[Drawing 8]

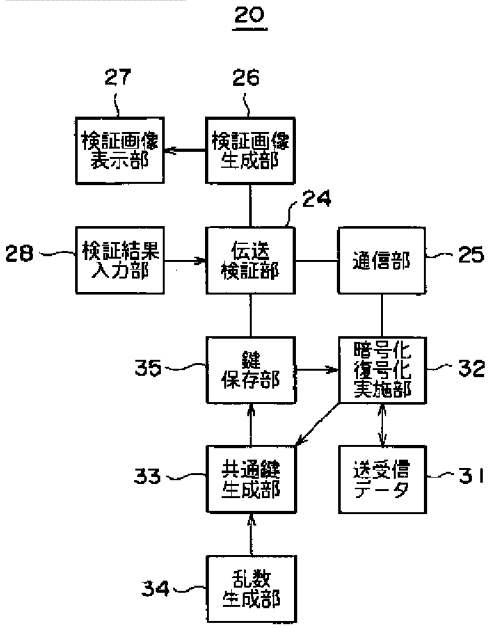
Type3



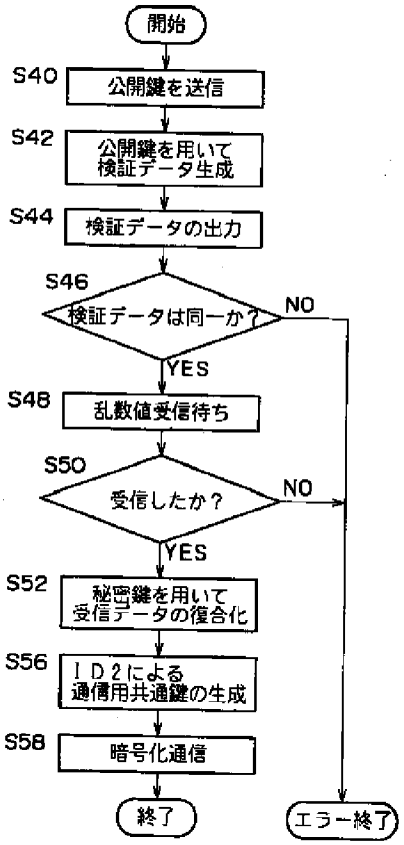
[Drawing 9]



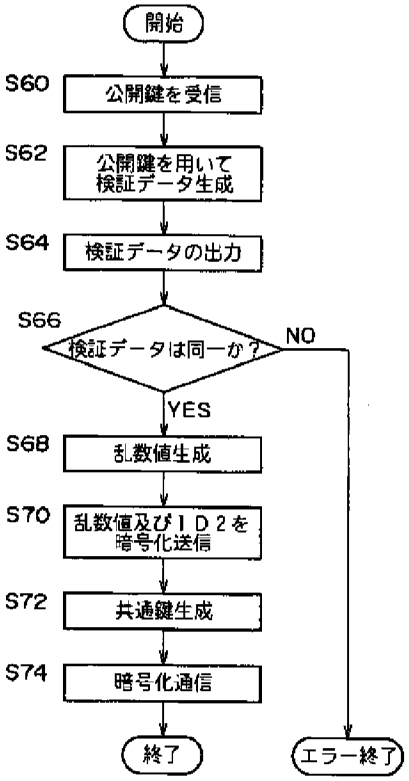
[Drawing 10]



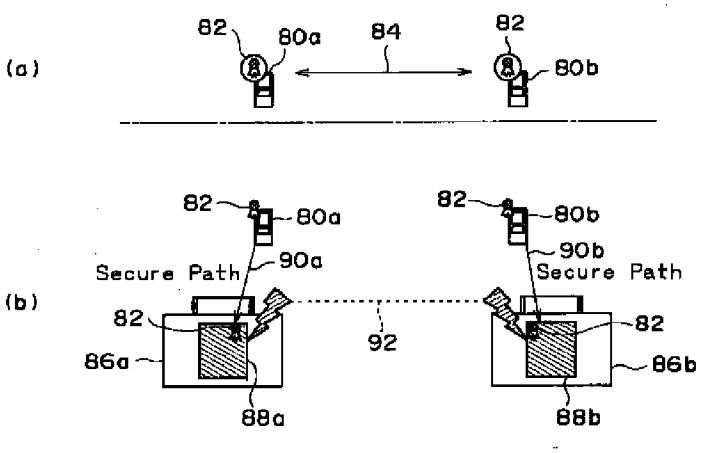
[Drawing 11]


開始
S40
公開鍵を送信
S42
公開鍵を用いて
検証データ生成
S44
検証データの出力
S46
検証データは同一か？
NO
YES
S48
乱数値受信待ち
S50
受信したか？
NO
YES
S52
秘密鍵を用いて
受信データの復合化
S56
ＩＤ２による
通信用共通鍵の生成
S58
暗号化通信
終了
エラー終了

[Drawing 12]


開始
S60
公開鍵を受信
S62
公開鍵を用いて
検証データ生成
S64
検証データの出力
S66
検証データは同一か？
NO
YES
S68
乱数値生成
S70
乱数値及びＩＤ２を
暗号化送信
S72
共通鍵生成
S74
暗号化通信
終了
エラー終了

[Drawing 13]



[Translation done.]